BayRS Version 14.00

Part No. 308643-14.00 Rev 00
September 1999

4401 Great America Parkway
Santa Clara, CA 95054

Configuring SMDS

NORTEL NETWORKS™

Copyright © 1999 Nortel Networks

All rights reserved. Printed in the USA. September 1999.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks is a registered trademark and ASN, BayRS, BayStack, and BayStream are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible

for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xi
Text Conventions xii
Acronyms xiii
Hard-Copy Technical Manuals xiv
How to Get Help xv

Chapter 1
SMDS Overview

How SMDS Sends LAN Data over WANs 1-2
SMDS Interface Protocol 1-2
Data Exchange Interface Protocol 1-4
PDU Assembly 1-4
SMDS Individual Addresses 1-7
SMDS Group Addresses 1-7
For More Information About SMDS 1-7

Chapter 2
Implementation Notes

Requirements for the Router and the DSU/CSU 2-3
DXI Protocol Requirements 2-3
Local Management Interface 2-3
Protocols Supported by SMDS 2-4
Priority of Heartbeat Poll Messages 2-4
Multinet 2-5
Multigroup 2-7
Configuring Synchronous Lines for SMDS 2-10

Chapter 3
Enabling SMDS

Using the MIB Object ID 3-1
Enabling SMDS on an Interface 3-2

Chapter 4
Editing SMDS Parameters

Editing SMDS Interface Parameters 4-2
SMDS Interface Parameter Descriptions 4-3
Deleting SMDS from the Router 4-7

Appendix A
SMDS Default Settings

Index

Figures

Figure 1-1. SMDS Sample Network 1-1
Figure 1-2. SMDS Interface Protocol Stack 1-3
Figure 1-3. SMDS Level-3 PDU 1-3
Figure 1-4. DXI Protocol 1-4
Figure 1-5. DXI Packet Assembly 1-6
Figure 2-1. Access to SMDS Network via a Router and DSU/CSU 2-1
Figure 2-2. Low-Speed Access to SMDS Network 2-2
Figure 2-3. Low-Speed Access to SMDS Network via a Low-Speed DSU 2-2
Figure 2-4. SMDS and IP Addresses for a Multinet Configuration 2-5
Figure 2-5. Multinet Configuration 2-6
Figure 2-6. Multigrouping SMDS and IP Addresses 2-7
Figure 2-7. Multigroup Configuration 2-9
Figure 3-1. SMDS Configuration Window 3-2
Figure 4-1. Configuration Manager Window 4-1
Figure 4-2. SMDS Interface List Window 4-2

Tables

Table 2-1. Synchronous Line Parameter Settings for SMDS 2-10
Table A-1. SMDS Interface Parameters A-1

Preface

If you are responsible for configuring and managing Nortel Networks™ routers or BayStream™ platforms, read this guide to learn how to customize Nortel Networks software for Switched Multimegabit Data Service (SMDS).

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`

separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CRC	Cyclic Redundancy Check
DSU/CSU	Digital Service Unit/Channel Service Unit
DS1	Digital Service, Level 1
DS3	Digital Service, Level 3
DXI	data exchange interface
HSSI	high-speed serial interface
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPX	Internet Packet Exchange
LAN	local area network
LMI	Local Management Interface
MAC	media access control
MAN	metropolitan area network
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First

PDU	protocol data unit
PVCs	permanent virtual circuits
RIP	Routing Information Protocol
SIP	SMDS Interface Protocol
SMDS	Switched Multimegabit Data Service
SNI	subscriber network interface
SNMP	Simple Network Management Protocol
WAN	wide area network
XNS	Xerox Network System

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Chapter 1
SMDS Overview

Switched Multimegabit Data Service (SMDS) is a public, high-speed, packet-switched network service that enables you to connect local area networks (LANs) across wide area networks (WANs). SMDS technology combines cell relay technology and IEEE Standard 802.6, the link control protocol standard that controls cell transmission. To send information across the network, SMDS divides data into fixed 53-byte cells. The use of cell technology makes SMDS well suited for traffic that consumes high bandwidth for short periods of time.

Figure 1-1 illustrates an SMDS network. In this illustration, LAN 1 communicates to LANs 2 and 3 through a router connected to an SMDS Digital Service Unit/Channel Service Unit (DSU/CSU). The DSU/CSU changes the frame-based data from the router into cells that can then be sent across the SMDS network.

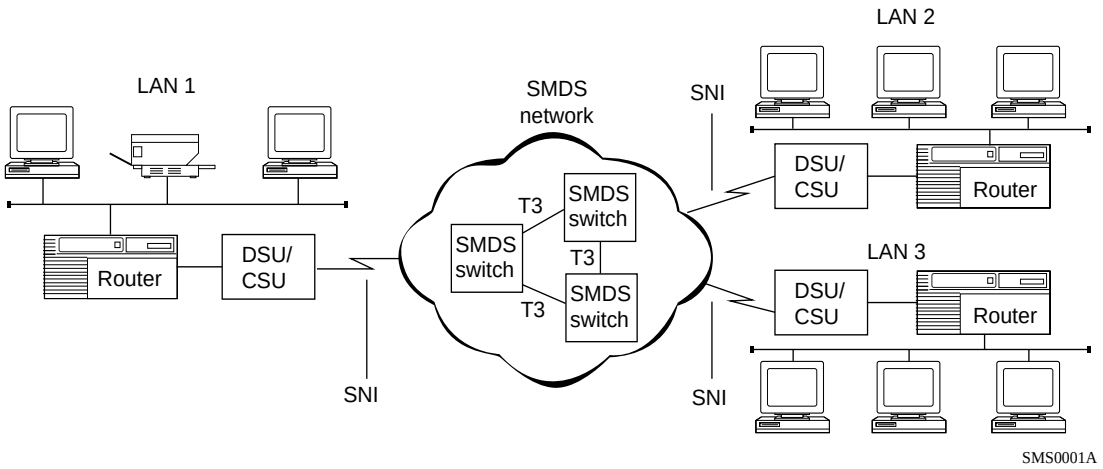

Figure 1-1. SMDS Sample Network

The point at which the DSU/CSU meets the network is the subscriber network interface (SNI). This is the access point to the SMDS network. Within the switching system of the SMDS network, T3 communication lines connect the network switches together.

Because data traffic and network equipment are different for each SMDS customer, SMDS defines several *access classes*. Access classes are speeds at which data travels from the customer site to the network switch.

SMDS currently offers six network access classes: 1.2 Mb/s, 4 Mb/s, 10 Mb/s, 16 Mb/s, 25 Mb/s, and 34 Mb/s. The 1.2 Mb/s class is for T1 lines. Classes 4 Mb/s through 34 Mb/s are for T3 lines. SMDS also offers low-speed SMDS classes, which operate at fractional T1/E1 speeds (56 Kb/s up to 64 Kb/s).

How SMDS Sends LAN Data over WANs

LAN data is typically connectionless data. This means that it has addressing information in each frame, so there is no need for a prior connection between the origination and destination devices. WAN data is typically connection-oriented data. This means that it needs a virtual circuit -- that is, a predefined path across physical lines -- between the two connection points prior to sending data. SMDS provides connectionless data transfer across a wide area network without establishing a logical end-to-end connection.

SMDS Interface Protocol

The SMDS Interface Protocol (SIP) defines SMDS addressing, formatting, framing, and error-detection requirements.

The SIP has three levels that are similar to, but do not match, the protocol layers that make up the OSI protocol model.

- Level 3 specifies the addressing, formatting, and encapsulation of packet data, referred to as Level-3 PDUs.
- Level 2 specifies the segmentation of Level-3 Protocol Data Units (PDUs) into short, fixed-length SMDS cells, referred to as Level-2 PDUs.
- Level 1 specifies the physical connectivity that enables transmission.

Figure 1-2 illustrates the SIP protocol stack.

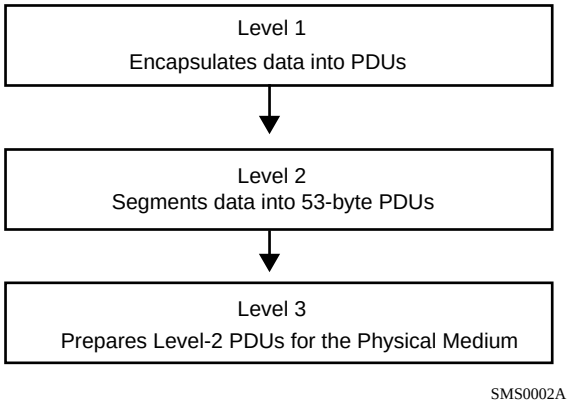

Figure 1-2. SMDS Interface Protocol Stack

SIP specifies that the SMDS source and destination addresses reside in the Level-3 PDU header (Figure 1-3). Each header contains a MAC-level address in an E.164 address format. E.164 formats are 64 bits long and provide both individual and multicast addresses. Network switches use the address information in the header to route the PDU to its destination.

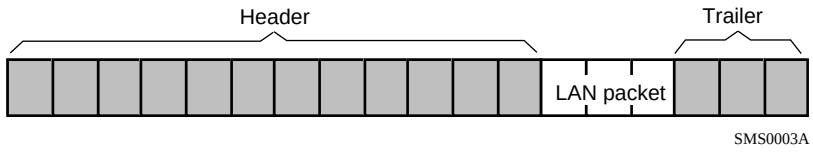

Figure 1-3. SMDS Level-3 PDU

One or more SMDS devices, for example DSUs and routers, can perform the tasks of the three SIP levels, as described in the next section.

Data Exchange Interface Protocol

For SMDS high-speed access classes, that is, speeds from 1.2 Mb/s to 34 Mb/s, the SMDS Interest Group (SIG) wanted to simplify the integration of SMDS into existing network equipment, and to hasten SMDS into the market. To do this, they divided the functions defined by the SIP levels between devices that handle local network packets (for example, a router) and devices that interface with the digital services provided by common carriers (a DSU/CSU).

The Data Exchange Interface (DXI) protocol defines this division of tasks and describes the router and DSU/CSU relationship (Figure 1-4). Refer to the next section for more information.

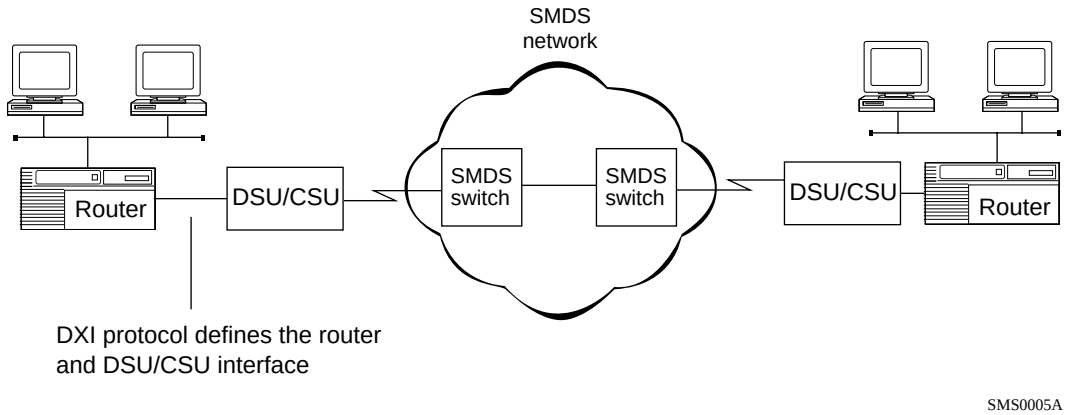

Figure 1-4. DXI Protocol

For low-speed SMDS (56 Kb/s to 64 Kb/s), the DXI is extended out to the SMDS network. In this case, you do not need a special SMDS DSU/CSU.

PDU Assembly

SMDS PDU assembly begins when the router receives a network-generated packet. The router takes the entire packet and encapsulates it within a 36-byte header (containing addressing, length, and control information) and a 4-byte trailer (containing a CRC value), thereby creating an SMDS Level-3 PDU (Figure 1-5).

The router next prepares the Level-3 PDU for transmission to the DSU/CSU by encapsulating it within a DXI header and trailer that provide control information. Upon receiving the DXI packet, the DSU/CSU strips the DXI header/trailer and divides the Level-3 PDU into fixed-length (44-byte) units called *cells*. The DSU/CSU encapsulates these cells within a 7-byte header and 2-byte trailer to form Level-2 PDUs.

Finally, the DSU/CSU inserts an additional four bytes of framing information between each Level-2 PDU and transmits the framed cells across a Digital Service Level 1 (DS1) or DS3 connection to the SMDS network.

Figure 1-5 shows the assembly of SMDS cells as specified by the DXI.

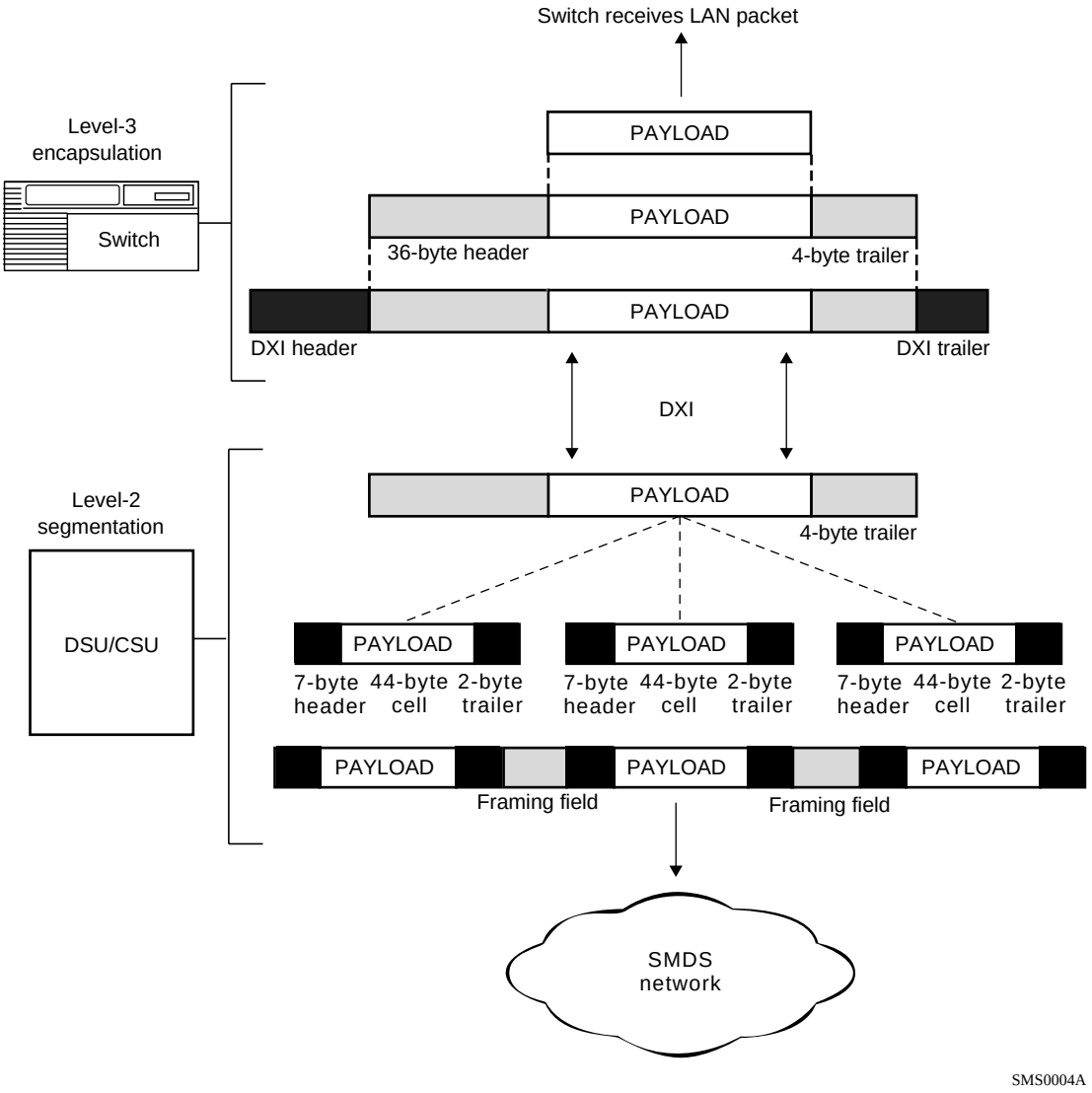

Figure 1-5. DXI Packet Assembly

SMDS Individual Addresses

An SMDS individual address is a unique address that the SMDS provider assigns to an SNI. Specifically, an individual address is a media access control layer (MAC) address in an E.164 format. An E.164 address is a 64-bit address, which for SMDS is similar to a phone number. For example, the phone number (617) 555-3923 becomes individual address C161 75 55 39 23 FF FF. The C indicates that the address is an individual address, and the 1 is a standard prefix. There can be up to 16 individual addresses for one SNI.

SMDS Group Addresses

An SMDS group address is one address that instructs an SMDS switch to broadcast information, such as routing information packets (RIP) and address resolution packets (ARP), from the router to multiple destination nodes. SMDS individual addresses within the SMDS group identify these nodes.

Like an SMDS individual address, the group address is a media access control layer (MAC) address in an E.164 format. An E.164 address is a 64-bit address, which for SMDS is similar to a phone number. For example, the phone number (508) 555-1144 becomes individual address E1 50 85 55 11 44 FF FF. The E indicates that the address is a group address and the 1 is a standard prefix.

For More Information About SMDS

The following documents provide technical details on SMDS and DXI protocol design and implementation:

Baker, F. and C. Kolb. *Definitions of Managed Objects for the DS1 Interface Type*. RFC 1232. Network Information Center (NIC), SRI International, Menlo Park, California, May 1991.

Bellcore. *Generic Requirements for SMDS Customer Network Management Service*. Technical Advisory TA-TSV-001062. Issue 2. February 1992.

Bellcore. *Generic System Requirements in Support of Switched Multi-Megabit Data Service*. Technical Reference TR-TSV-000772. Issue 1. May 1991.

Bellcore. *Local Access System Generic Requirements, Objectives, and Interfaces in Support of Switched Multi-Megabit Data Service.* Technical Reference TR-TSV-000773. Issue 1. June 1991.

Cox, T. and K. Tesink. *Definitions of Managed Objects for the DS3 Interface Type*. RFC 1233. Network Information Center (NIC), SRI International, Menlo Park, California, May 1991.

Klessig, R. and K. Tesink. *SMDS: Wide-Area Data Networking with Switched Multi-megabit Data Service*. Englewood, New Jersey: Prentice Hall, Inc., 1995.

Piscitello, D. and J. Lawrence. *The Transmission of IP Datagrams over the SMDS Service*. RFC 1209. Network Information Center (NIC), SRI International, Menlo Park, California, March 1991.

SMDS Interest Group. *SMDS Data Exchange Interface Protocol*. Revision 3.2. Technical Specification SIG-TS-001/1991. October 1991.

SMDS Interest Group. *SMDS DXI Local Management Interface.* Technical Specification SIG-TS-002/1992. May 1992.

The following publications provide a less technical introduction to SMDS:

Davidson, R. and N. Muller. *The Guide to SONET: Planning, Installing & Maintaining Broadband Networks*. Telecom Library, Inc., 1991.

Goldstein, F. *ISDN in Perspective*. Reading, Mass.: Addison-Wesley, 1992.

Chapter 2
Implementation Notes

This chapter provides information about the Nortel Networks implementation of SMDS. Specifically, it contains information about the router's DXI protocol requirements and the Local Management Interface protocol. This chapter also supplies details on the use of SMDS group and individual addresses for multinet and multigroup configurations.

To implement high-speed SMDS, you need a Nortel Networks router and an SMDS DSU/CSU that provides DS1- or DS3-based access to the switched SMDS network. A synchronous or high-speed serial interface (HSSI) physically connects the router and the DSU/CSU (Figure 2-1).

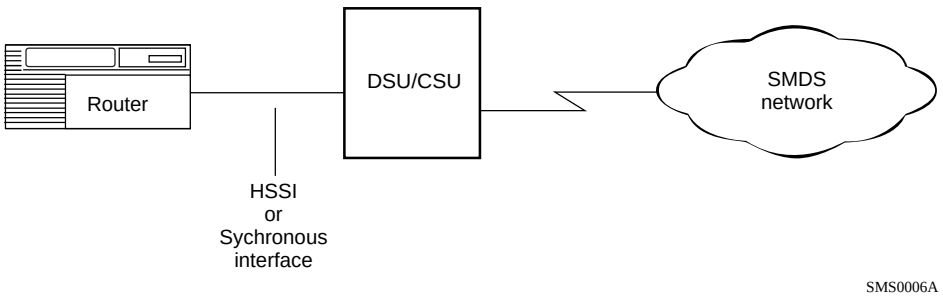

Figure 2-1. Access to SMDS Network via a Router and DSU/CSU

The router also supports low-speed SMDS through the SNI and DXI specifications standardized by the SMDS Interest Group. If you are running low-speed SMDS, you can extend the DXI to the SMDS network, thereby eliminating the need for a special SMDS DSU/CSU. Any synchronous interface, including MCT1 or MCE1 link modules, physically connects the router and the network (Figure 2-2).

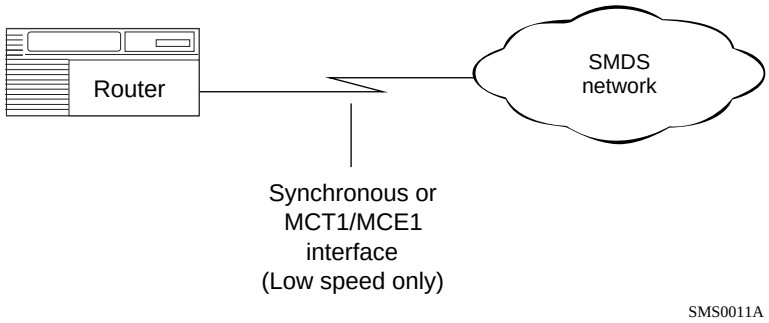

Figure 2-2. Low-Speed Access to SMDS Network

Another low-speed SMDS option is to use a low-speed DSU/CSU to connect to the network. In this case, a V.35 cable physically connects the router to the DSU/CSU (Figure 2-3).

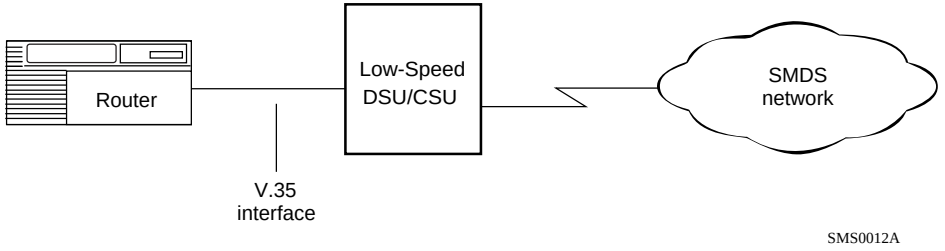

Figure 2-3. Low-Speed Access to SMDS Network via a Low-Speed DSU

Requirements for the Router and the DSU/CSU

The next sections provide configuration requirements for the router and the DSU/CSU to implement high-speed SMDS.

DXI Protocol Requirements

Version 3.2 of the DXI protocol manages the data exchange between the router and the DSU/CSU. Because the router does not support earlier DXI versions, the DSU/CSU must support DXI Version 3.2. DXI Version 3.2 provides an optional *heartbeat poll* mechanism to periodically verify the router and DSU/CSU connection. Be sure to enable heartbeat polling on the DSU/CSU.

The DXI also provides support for both 16-bit and 32-bit cyclic-redundancy checks (CRCs). Network devices use CRCs to check data for transmission errors. When the router or DSU/CSU receives data, each reads the CRC character and compares the value it calculates to the actual CRC character in the data packet.

Ensure that the CRC values for the router and the DSU/CSU match. This means that if you set the router to 16-bit CRCs, you must set the DSU/CSU to 16-bit CRCs. If necessary, you can modify the CRC values (16-bit or 32-bit) for both synchronous and HSSI connections.

Local Management Interface

The Local Management Interface (LMI) protocol works with the DXI to enable the router and the DSU/CSU to exchange management information. The LMI uses a subset of the Simple Network Management Protocol (SNMP) to provide for router management queries, DSU/CSU responses to queries, and DSU/CSU-generated asynchronous trap events.

Before enabling the LMI on the router, ensure that the DSU/CSU supports this protocol and that you enable it on the DSU/CSU.

Protocols Supported by SMDS

SMDS can operate with the following protocols:

- AppleTalk
- APPN
- Bridge (including Spanning Tree)
- DECnet IV
- DLSw
- Internet Protocol (IP), including Address Resolution Protocol (ARP) support
- Internet Packet Exchange (IPX)
- LLC2
- Native Mode LAN
- Source Routing with Nortel Networks 8101 encapsulation
- Source Routing with Spanning Tree
- VINES
- Xerox Network System (XNS)

Note: SMDS does not support OSI.

Priority of Heartbeat Poll Messages

When you select SMDS on a circuit, the router automatically assigns the highest priority to heartbeat poll and LMI messages that it sends to the DSU/CSU. The heartbeat poll and LMI messages must have priority over other data to ensure that during heavy traffic conditions, the link stays up and allows these messages to get through to the DSU/CSU.

Multinet

Multinet, a feature of the Internet Protocol (IP), allows you to support many IP networks over one SMDS line by allowing many hosts on a single logical IP subnetwork. A multinet network is economical because you do not have to purchase as many SMDS group addresses from your SMDS provider as you might with other configurations.

Multinet configurations enable you to configure one SMDS individual address and one SMDS group address for a single SNI and then associate many logical IP subnetworks with these single SMDS addresses. A logical IP subnetwork is a host that is directly connected to the SMDS network.

A second variation of a multinet configuration allows you to have multiple SMDS individual addresses along with a single SMDS group address by configuring an individual address per IP host address for the same group address. For information about IP, refer to *Configuring IP Services.*

Figure 2-4 shows the two types of multinet configurations.

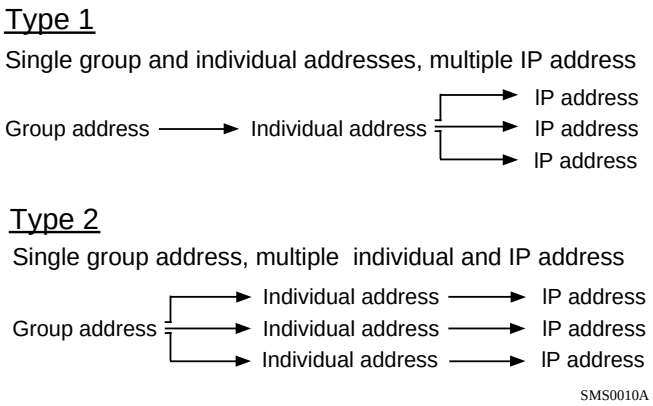

Figure 2-4. SMDS and IP Addresses for a Multinet Configuration

Figure 2-5 on page 2-6 shows a sample multinet configuration, where several IP networks are using one SNI. Each side of the network shows a different use of group and individual addresses for connecting to the IP networks. A multinet configuration allows for efficient network addressing and a cost-effective method of implementing SMDS.

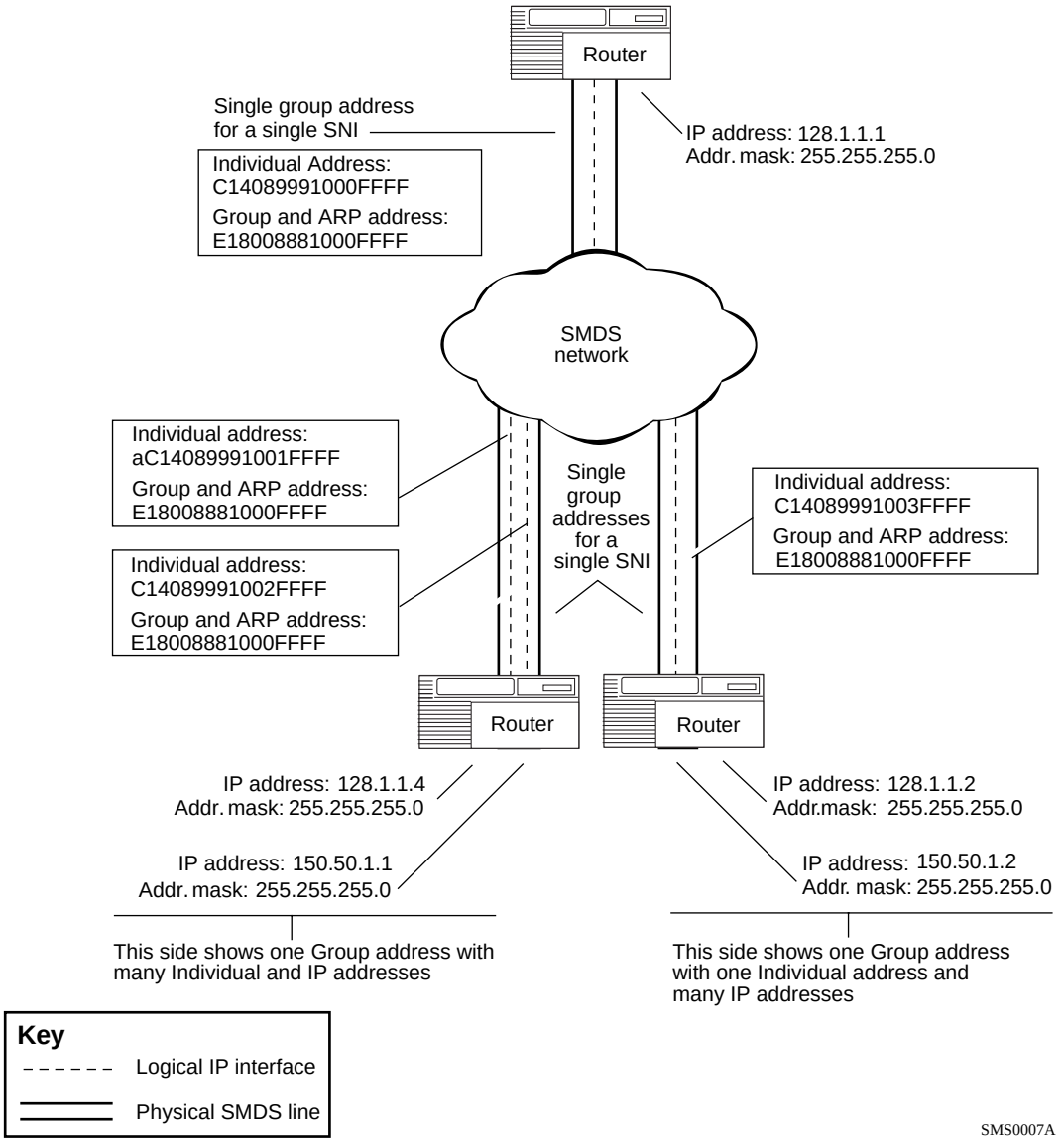

Figure 2-5. Multinet Configuration

To configure multinet, follow these steps:

1. **In your SMDS configuration parameters, enter addresses in the Group Address, ARP Address, and Individual Address parameters described in Chapter 3 of this book.**
2. **In your IP interface configuration, enter the same addresses that you entered in the SMDS parameters in the previous step.**

   The equivalent IP parameters are SMDS Group Address, SMDS ARP Req Address, and MAC Address. Refer to *Configuring IP Services* for information about these IP parameters.
3. **Add a new IP interface with a unique IP address, which includes a network/subnet and host address.**
4. **Enter the same Group Address, ARP Address, and Individual Address that you entered in Step 2 for this new IP interface.**

Note: You may also configure many individual addresses for an SMDS group address, but ensure that each individual address within a group is unique.

Multigroup

Multigroup is a feature of the Internet Protocol (IP) that enables you to configure multiple SMDS group addresses on the same SNI, which is the access interface to the SMDS network. The router implements multigroup according to RFC 1209. For information about IP, refer to *Configuring IP Services.*

Figure 2-6 shows a multigroup configuration.

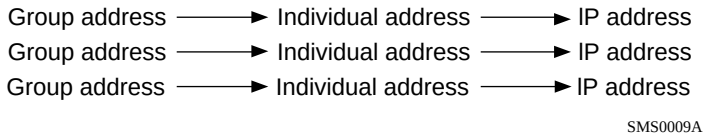
Group address → Individual address → IP address
Group address → Individual address → IP address
Group address → Individual address → IP address
SMS0009A

Figure 2-6. Multigrouping SMDS and IP Addresses

Once you configure an SMDS group address, you can then assign this group address to at least one IP subnetwork. An IP address identifies the subnetwork.

By associating or *pairing* a different SMDS group address with each IP address, you achieve multigrouping. A multigroup configuration enables you to use one SMDS physical line (SNI) to connect many nodes located on different subnetworks. It also allows you to limit broadcast and multicast traffic, such as Routing Information Protocol (RIP) updates, Address Resolution Protocol (ARP) updates, and Open Shortest Path First (OSPF) messages, to their respective SMDS groups.

For example, in Figure 2-7, two separate subnetworks share the same SNI. The routers in these networks use RIP updates to communicate network information. The routers broadcast RIP updates to each node on the network. Because each RIP network shares an SNI, the only way to prevent RIP updates from interfering with one another is to isolate these subnetworks by associating each one with a different SMDS group address.

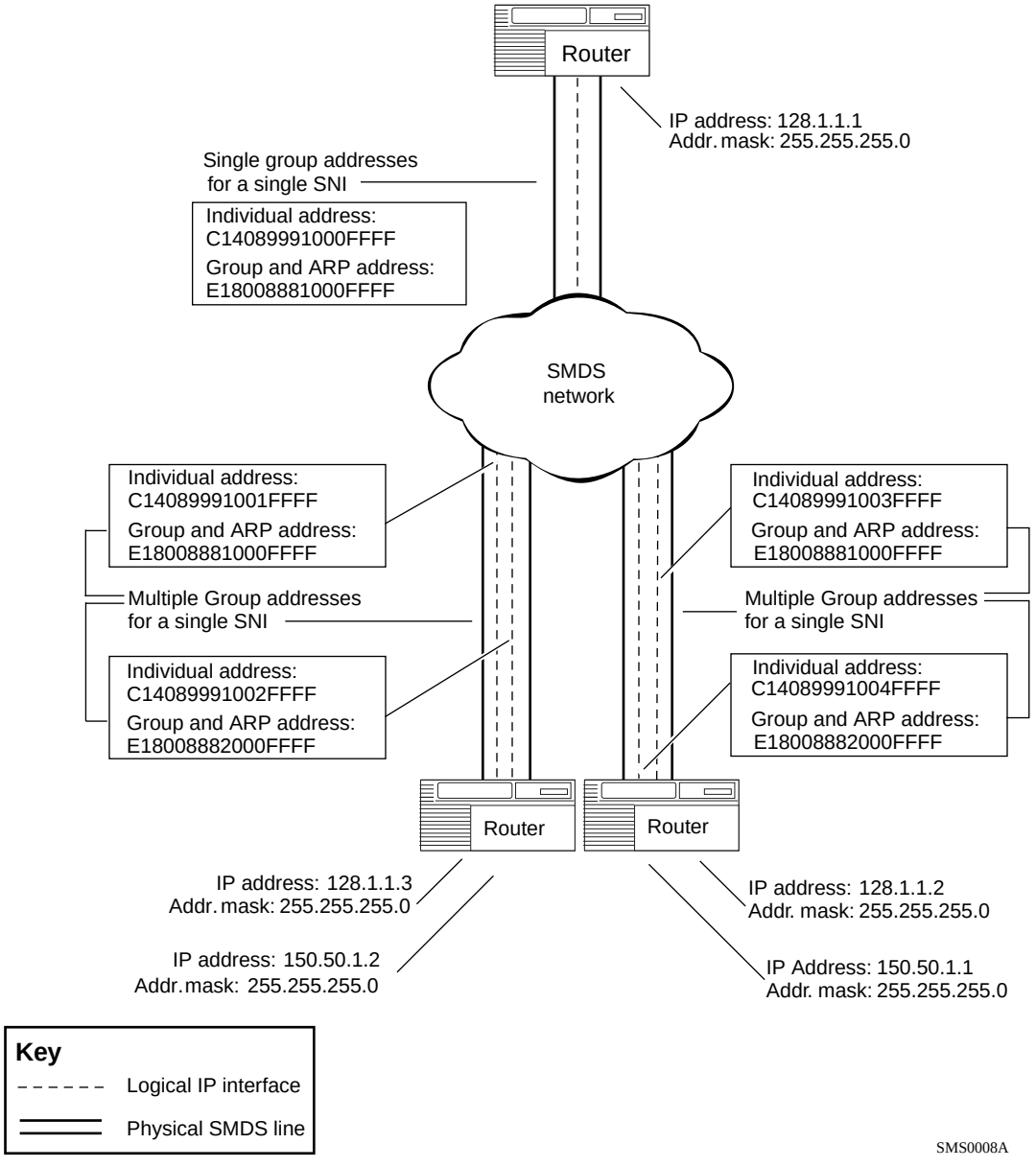

Figure 2-7. Multigroup Configuration

To configure multigroup, follow these steps:

1. **In your SMDS configuration parameters, enter addresses in the Group Address, ARP Address, and Individual Address parameters described in Chapter 3 of this book.**
2. **In your IP interface configuration, enter the same addresses that you entered in the SMDS parameters in the previous step.**

   The equivalent IP parameters are SMDS Group Address, SMDS ARP Req Address, and MAC Address. Refer to *Configuring IP Services* for information about these IP parameters.
3. **Add a new IP interface with a unique IP subnetwork address. This address should include a network/subnet and host address.**
4. **Enter a new Group Address, ARP Address, and Individual Address for this new IP interface.**

   The IP interface parameters override these same parameters in the SMDS configuration for this and subsequent IP interfaces.

Configuring Synchronous Lines for SMDS

If you enable SMDS on a circuit, Site Manager automatically sets the following synchronous line parameters.

Table 2-1. Synchronous Line Parameter Settings for SMDS

Parameter	Value
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	SMDS

For more information about these parameters, refer to *Configuring and Managing Routers with Site Manager.*

Chapter 3
Enabling SMDS

This chapter provides information on how to enable SMDS. It assumes you have read *Configuring and Managing Routers with Site Manager* and that you have

1. Opened a configuration file
2. Specified router hardware, if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling SMDS

When you enable SMDS, you need to configure only a few parameters. The Configuration Manager supplies default values for the remaining parameters. If you want to edit these default values, refer to Chapter 4 for instructions.

Using the MIB Object ID

For each parameter, this chapter and Chapter 4 include path, default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Enabling SMDS on an Interface

To enable SMDS on an interface, complete the following steps:

1. **Select SMDS from the WAN Protocols menu; this menu appears after you select a link or net module connector that requires a WAN circuit.**

   Site Manager automatically enables protocol prioritization when you select SMDS. For detailed information on protocol prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization.*

2. **Click on OK to enable default SMDS.**

   The Configuration Manager displays the SMDS Configuration window (Figure 3-1).

3. **Configure the SMDS parameters (Individual Address, Group Address, and ARP Address) using the descriptions that follow as a guide.**

4. **When you have configured all the parameters, you can do one of the following:**

   - Enable default SMDS. To do this, click on OK.
   - Edit the default values. To do this, click on Details. (Refer to Chapter 4 for instructions.)

Figure 3-1. SMDS Configuration Window

Parameter:	**Individual Address**
Path:	Configuration Manager > Protocols > SMDS
Default:	C1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides a MAC-layer address.
Instructions:	Enter the complete SMDS E.164 address; for example, C15085558734FFFF. To configure this parameter for a multigroup or multinet configuration, refer to Chapter 2 for instructions. For information about IP, refer to *Configuring IP Services.*
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.5

Parameter:	**Group Address**
Path:	Configuration Manager > Protocols > SMDS
Default:	E1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides a MAC-layer multicast address for this SMDS interface.
Instructions:	Enter the complete SMDS E.164 group address, for example, E16175552876FFFF. To configure this parameter for a multigroup or multinet configuration, refer to Chapter 2 for instructions. For information about IP, refer to *Configuring IP Services.*
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.6

Parameter:	**ARP Address**
Path:	Configuration Manager > Protocols > SMDS
Default:	E1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides an address resolution multicast address.
Instructions:	Enter the complete SMDS E.164 address, for example, E16175552876FFFF. To configure this parameter for a multigroup or multinet configuration, refer to Chapter 2 for instructions. For information about IP, refer to *Configuring IP Services.*
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.7

Chapter 4
Editing SMDS Parameters

This chapter tells you how to edit SMDS parameters for the SMDS interfaces on your router.

Note: You must have already configured at least one SMDS interface on the router to edit SMDS parameters. If you have not yet done this, or want to add more interfaces, see *Configuring and Managing Routers with Site Manager.*

Access SMDS parameters from the Configuration Manager window (Figure 4-1). See *Configuring and Managing Routers with Site Manager* for instructions on how to access this window.

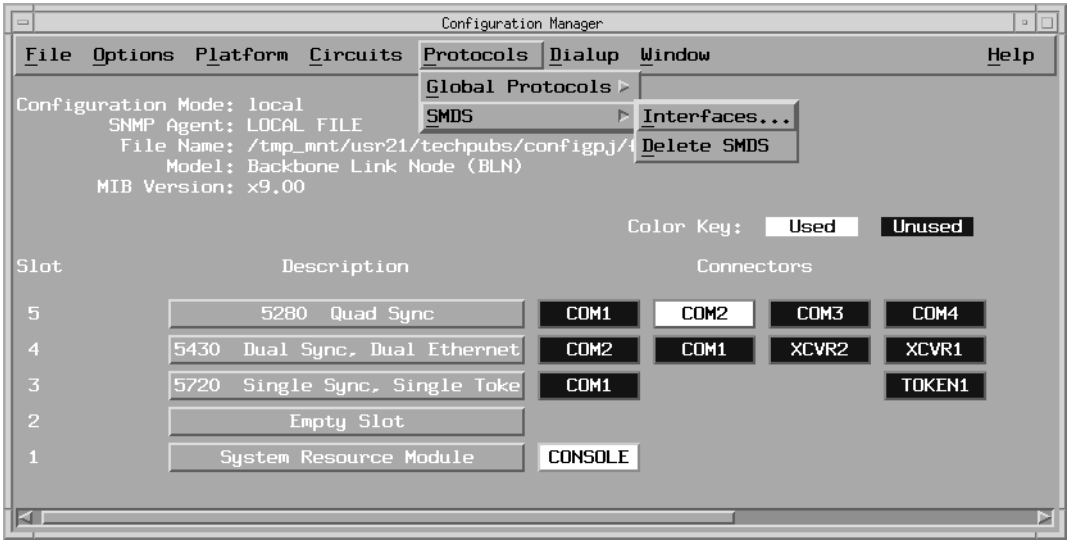

Figure 4-1. Configuration Manager Window

Editing SMDS Interface Parameters

To edit SMDS interface parameters, follow these steps:

1. **Begin at the Configuration Manager window (Figure 4-1).**
2. **Select Protocols > SMDS > Interfaces.**

   The Configuration Manager displays the SMDS Interface List window (Figure 4-2).

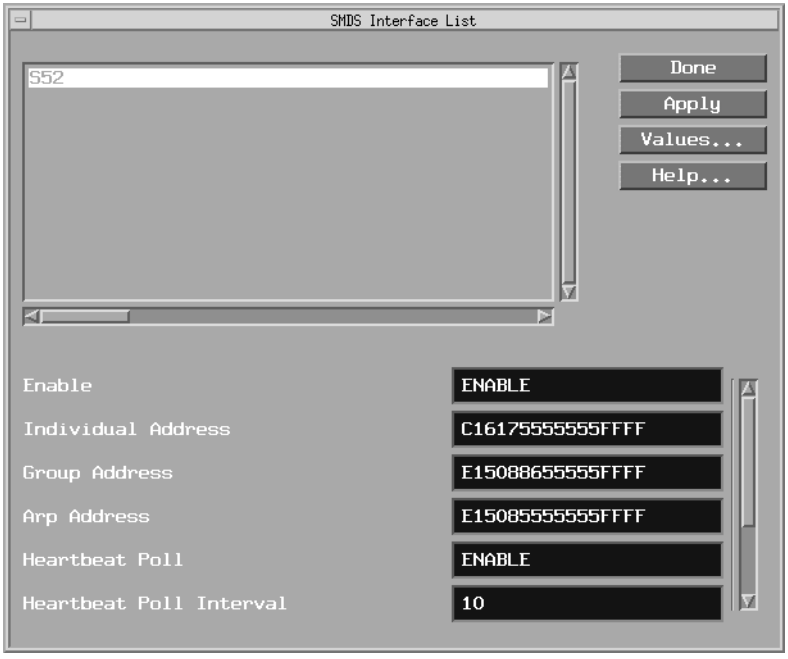

Figure 4-2. SMDS Interface List Window

3. **Select the interface you want to edit from the scroll box in the SMDS Interface List window.**
4. **Edit the parameters, referring to the parameter descriptions following this procedure.**
5. **Click on Apply to save your changes when you are finished. Repeat Steps 3 through 5 for each SMDS interface you want to edit.**
6. **Click on Done to exit.**

SMDS Interface Parameter Descriptions

Use the following descriptions as guidelines when you edit the SMDS interface parameters.

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables SMDS on this interface.
Instructions:	Set to Disable if you want to temporarily disable SMDS on this interface, rather than delete it. Set this parameter to Enable if you want to re-enable SMDS.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.2

Parameter:	**Individual Address**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	C1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides a MAC-layer address. The Configuration Manager fills in this field based on your original SMDS interface configuration.
Instructions:	Enter the new SMDS E.164 address, for example, C15085558734FFFF. To configure this parameter for a multinet or multigroup configuration, refer to Chapter 2 for instructions.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.5

Parameter:	**Group Address**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	E1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides a MAC-layer multicast address for this SMDS interface. The Configuration Manager fills in this field based on your original SMDS interface configuration.
Instructions:	Enter the new SMDS E.164 group address, for example, E16175552876FFFF. To configure this parameter for a multinet or multigroup configuration, refer to Chapter 2 for instructions.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.6

Parameter:	**ARP Address**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	E1FFFFFFFFFFFFF
Options:	A complete SMDS E.164 address specified by the SMDS subscription agreement that you have with your SMDS provider
Function:	Provides an address resolution multicast address. The Configuration Manager fills in this field based on your original SMDS interface configuration.
Instructions:	Enter the new SMDS E.164 address, for example, E16175552876FFFF. To configure this parameter for a multinet or multigroup configuration, refer to Chapter 2 for instructions.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.7

Parameter:	**Heartbeat Poll**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables DXI heartbeat polling. DXI Version 3.2 provides a heartbeat polling mechanism, which verifies the integrity of the router/DSU connection. To implement heartbeat polling, the router transmits a constant stream of keep-alive messages to the DSU. The DSU, in turn, sends an acknowledgment to the router.
Instructions:	Set to Enable to enable heartbeat polling. Set to Disable if the DSU/CSU in your network does not support heartbeat polling.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.8

Parameter:	**Heartbeat Poll Interval**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	10 seconds
Range:	6 to 1023 seconds
Function:	Specifies the time interval between each heartbeat poll message that the router transmits. If you disable heartbeat polling, this parameter is nonfunctional.
Instructions:	Enter the number of seconds between the transmission of heartbeat poll messages. Be sure to set this parameter to a value greater than 5 seconds, the length of the heartbeat poll acknowledgment timer. We recommend that you accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.9

Parameter:	**Heartbeat Poll Down Count**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	3 messages
Range:	1 to 1023 messages
Function:	Specifies the number of heartbeat poll messages that the router will send without acknowledgment from the DSU before it declares the router/DSU connection down. If you disable heartbeat polling, this parameter is nonfunctional.
Instructions:	Set to the number of unacknowledged heartbeat poll messages that the router will tolerate before taking the router/DSU connection down. We recommend that you accept the default.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.10

Parameter:	**LMI Network Mgmt**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables LMI network management. LMI works with DXI Version 3.2. LMI is an SNMP-like protocol that enables the router and the DSU/CSU to exchange management information.
Instructions:	Set to Enable to use the LMI protocol. Accept the default, Disable, if the DSU/CSU in your network does not support the LMI. Accept the default if you have an ADC Kentrox dual-port DataSMART T1 SMDSU. This DSU does not support the LMI protocol. Instead, rely on heartbeat polling to determine whether the interface between the router and the DSU is active. Use the SMDS in-band SNMP agent to manage the DSU. If you have a single-port DataSMART T1 SMDSU, accept the default or upgrade the DSU software to revision 1.41, which supports LMI.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.11

Parameter:	**Enable Incoming Address Screening**
Path:	Configuration Manager > Protocols > SMDS > Interfaces
Default:	Disable
Options:	Enable | Disable
Function:	Enables the router to verify the individual and group addresses that it receives in the incoming frames and drop any improperly addressed frames. It ensures that the router receives only traffic intended for it. If the router rejects an address, one of three things may be happening: • You did not configure the SMDS addresses according to the numbers the service provider assigned. • The network is forwarding traffic to the router unnecessarily. Notify the network provider. • If the router shares a network entry point with another device, the router may be receiving that device's traffic.
Instructions:	Set to Enable if you want the router to check incoming addresses and control the calls it receives. If not, accept the default, Disable. To determine whether the router is rejecting addresses, use the Technician Interface script **show smds stats.** Refer to *Using Technician Interface Scripts* for more information.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.3.1.17

Deleting SMDS from the Router

To delete SMDS from all router circuits, complete the following steps:

1. **From the Configuration Manager window (refer to Figure 4-1), select Protocols > SMDS > Delete SMDS.**

   The Configuration Manager prompts

   ```
   Do you REALLY want to delete SMDS?
   ```

2. **Click on OK.**

   The Configuration Manager returns you to the Configuration Manager window. SMDS is no longer configured on the router.

Appendix A
SMDS Default Settings

This appendix lists the default settings for SMDS. Use the Configuration Manager to edit any of the default settings listed here.

Table A-1. SMDS Interface Parameters

Parameter	Default
Enable	Enable
Individual Address	C1FFFFFFFFFFFFF
Group Address	E1FFFFFFFFFFFFF
ARP Address	E1FFFFFFFFFFFFF
Heartbeat Poll	Enable
Heartbeat Poll Interval	10 seconds
Heartbeat Poll Down Count	3 messages
LMI Network Mgmt	Disable
Enable Incoming Address Screening	Disable

Index

A

access classes for SMDS, 1-2
acronyms, xiii
addresses
  group, 1-7
    used for multigroup, 2-7
    used for multinet, 2-5
  individual, 1-7
    used for multigroup, 2-7
    used for multinet, 2-5
ARP Address parameter, 3-4, 4-4

C

connections to router, 2-1
connectivity using heartbeat polling, 2-3
conventions, text, xii
customer support, xv
cyclic-redundancy check (CRC) values, 2-3

D

Data Exchange Interface (DXI) protocol
  description, 1-4
  requirements for SMDS
    version supported, 2-3
defaults for SMDS parameters, A-1
deleting SMDS from the router, 4-7
DSU/CSU
  configuration requirements for, 2-3
  role in SMDS network, 1-4

E

E.164 addresses for SMDS, 1-3
Enable Incoming Address Screening parameter, 4-7
Enable parameter, 4-3
enabling SMDS, 3-1 to 3-4

G

Group Address parameter, 3-3, 4-4

H

Heartbeat Poll Down Count parameter, 4-6
Heartbeat Poll Interval parameter, 4-5
heartbeat poll messages, 2-4
Heartbeat Poll parameter, 4-5
heartbeat polling for connections, 2-3
high-speed serial interface (HSSI) connections, 2-1
high-speed SMDS
  description, 1-2
  implementing, 2-1

I

IEEE Standard 802.6 used by SMDS, 1-1
implementation notes, 2-1 to 2-10
Individual Address parameter, 3-3, 4-3
information sources on SMDS, 1-7

L

line configuration. *See* synchronous line configuration

LMI Network Mgmt parameter, 4-6

Local Management Interface (LMI)
- enabling, 4-6
- purpose of, 2-3

low-speed SMDS
- description of, 1-2
- implementing, 2-1

M

MIB object ID, 3-1

multigroup
- description, 2-7
- sample configuration, 2-8
- setting parameters for, 2-10

multinet
- description, 2-5
- sample configuration, 2-5
- setting parameters for, 2-7

P

parameters
- ARP Address, 3-4, 4-4
- editing, 4-1 to 4-7
- Enable, 4-3
- Enable Incoming Address Screening, 4-7
- Group Address, 3-3, 4-4
- Heartbeat Poll, 4-5
- Heartbeat Poll Down Count, 4-6
- Heartbeat Poll Interval, 4-5
- Individual Address, 3-3, 4-3
- LMI Network Mgmt, 4-6

product support, xv

protocol data unit (PDU)
- assembly, 1-4
- definition, 1-2

protocols supported by SMDS, 2-4

publications, hard copy, xiv

R

router requirements for SMDS, 2-3

S

SMDS
- access classes description, 1-2
- addresses, 1-7
- defaults, A-1
- deleting from the router, 4-7
- enabling, 3-1 to 3-4
- implementation notes, 2-1 to 2-10
- information sources, 1-7
- LMI, 2-3
- overview of, 1-1 to 1-7
- router requirements for, 2-3
- sending data over WANs, 1-2
- supported protocols, 2-4

SMDS Interface Protocol (SIP)
- definition, 1-2

speeds for SMDS, 1-2

subscriber network interface (SNI) definition, 1-2, 2-1

support, Nortel Networks, xv

Switched Multi-megabit Data Service. *See* SMDS

synchronous line configuration, 2-10

T

technical publications, xiv

technical support, xv

text conventions, xii